SUBMITTAL TO THE BOARD OF SUPERVISORS
COUNTY OF RIVERSIDE, STATE OF CALIFORNIA

ITEM: 2.9
(ID # 19456)
MEETING DATE:
Tuesday, July 12, 2022

FROM : AUDITOR CONTROLLER:

SUBJECT: AUDITOR-CONTROLLER: Internal Audit Report 2022-020 Riverside County Information Technology Audit

RECOMMENDED MOTION: That the Board of Supervisors:

1. Receive and file Internal Audit Report 2022-020: Riverside County Information Technology Audit

ACTION:Consent

Tanya Harris
Tanya Harris, Assistant Auditor Controller 6/23/2022

MINUTES OF THE BOARD OF SUPERVISORS

On motion of Supervisor Jeffries, seconded by Supervisor Hewitt and duly carried, IT WAS ORDERED that the above matter is received and filed as recommended.

Ayes:	Jeffries, Washington and Hewitt
Nays:	Spiegel
Absent:	Perez
Date:	July 12, 2022
xc:	Auditor, RCIT

Kecia R. Harper
Clerk of the Board
By: _____
Deputy

SUBMITTAL TO THE BOARD OF SUPERVISORS COUNTY OF RIVERSIDE, STATE OF CALIFORNIA

FINANCIAL DATA	Current Fiscal Year:	Next Fiscal Year:	Total Cost:	Ongoing Cost
COST	$ 0	$ 0	$ 0	$ 0
NET COUNTY COST	$ 0	$ 0	$ 0	$ 0
SOURCE OF FUNDS: N/A			Budget Adjustment: No	
			For Fiscal Year: N/A	

C.E.O. RECOMMENDATION: Approve.

BACKGROUND:

Summary

In accordance with Board of Supervisors Resolution 83-338, we audited the Riverside County Information Technology department to provide management and the Board of Supervisors with an independent assessment of internal controls over application controls, billing for services, device disposal, and software licensing maintenance.

Our conclusion and details of our audit are documented in the body of this audit report.

Impact on Residents and Businesses

Provide an assessment of internal controls over the audited areas.

SUPPLEMENTAL:

Additional Fiscal Information

Not applicable

ATTACHMENTS:

A: Riverside County Auditor-Controller's Office - Internal Audit Report 2022-020: Riverside County Information Technology Audit

Internal Audit Report 2022-020

Riverside County
Information Technology
Audit

Report Date: July 12, 2022

AUDITOR CONTROLLER
COUNTY OF RIVERSIDE

Office of Paul Angulo, CPA, MA
Riverside County Auditor-Controller
4080 Lemon Street, 11th Floor
Riverside, CA 92509
(951) 955-3800

www.auditorcontroller.org

COUNTY OF RIVERSIDE
OFFICE OF THE
AUDITOR-CONTROLLER

County Administrative Center
4080 Lemon Street, 11th Floor
P.O. Box 1326
Riverside, CA 92502-1326
(951) 955-3800
Fax (951) 955-3802

AUDITOR CONTROLLER
COUNTY OF RIVERSIDE

Paul Angulo, CPA, MA
Riverside County Auditor-Controller

Tanya S. Harris, DPA, CPA
Assistant Auditor-Controller

July 12, 2022

Jim Smith
Chief Information Officer
Riverside County Information Technology
3450 14th Street
Riverside, CA 92501

Subject: **Internal Audit Report 2022-020: Riverside County Information Technology Audit**

Dear Mr. Smith:

In accordance with Board of Supervisors Resolution 83-338, we audited the Riverside County Information Technology department to provide management and the Board of Supervisors with an independent assessment of internal controls over application controls, device disposal, and software licensing maintenance.

We conducted our audit in accordance with the International Standards for the Professional Practice of Internal Auditing. These standards require that we plan and perform the audit to obtain sufficient, reliable, relevant and useful information to provide reasonable assurance that our objective as described above is achieved. An internal audit includes the systematic analysis of information to evaluate and improve the effectiveness of internal controls. We believe this audit provides a reasonable basis for our conclusion.

Internal controls are processes designed to provide management reasonable assurance of achieving efficiency of operations, compliance with laws and regulations, and reliability of financial and non-financial information. Management is responsible for establishing and maintaining adequate internal controls. Our responsibility is to evaluate the internal controls.

Our conclusion and details of our audit are documented in the body of this audit report.

AUDITOR CONTROLLER
COUNTY OF RIVERSIDE

Internal Audit Report 2022-020: Riverside County Information Technology Audit

As requested, in accordance with paragraph III.C of the Board of Supervisors Resolution 83-338, management responded to each reported condition and recommendation contained in our report. Management's responses are included in the report. We will follow-up to verify that management implemented the corrective actions.

Paul Angulo, CPA, MA
Riverside County Auditor-Controller

By: René Casillas, CPA, CRMA
Chief Internal Auditor

cc: Board of Supervisors
Jeff A. Van Wagenen, Jr., County Executive Officer
Dave Rogers, Chief Administrative Officer
Grand Jury

Table of Contents

Executive Summary

Overview

Riverside County Information Technology (Information Technology) is responsible for serving county departments, elected officials, and the public with a wide variety of information technology services. Information Technology is responsible for planning, designing, implementing, operating, and coordinating the county's information technology systems and networks, and for the delivery of information processing and communications services.

Riverside County Information Technology has an adopted budget of $98.7 million for FY 2021-22 and 397 adopted positions to execute its responsibilities. *County of Riverside, Fiscal Year 2021-22 Adopted Budget Volume 1, 196-197.*

Audit Objective

Our objective is to provide management and the Board of Supervisors with an independent assessment about the adequacy and effectiveness of internal controls over application controls, device disposal, and software licensing. Internal controls are processes designed to provide management reasonable assurance of achieving efficiency of operations, compliance with laws and regulations, and reliability of financial and non-financial information. Reasonable assurance recognizes internal controls have inherent limitations, including cost, mistakes, and intentional efforts to bypass internal controls. support

Audit Scope and Methodology

We conducted the audit from December 27, 2021, through April 26, 2022, for operations from July 1, 2020, through February 20, 2022. Following a risk based approach, our scope initially included the following:

- Application Controls
- Billing for Services
- Device Disposal
- Software Licensing Maintenance

Through inquiry, observations, and limited examination of relevant documentation, it was determined through a risk assessment of the business processes for billing for

services, that the risk exposure to the Information Technology associated with these processes are well mitigated with internal controls and are functioning as designed. Therefore, we focused our audit scope to internal controls over application controls, device disposal, and software licensing maintenance.

Audit Highlights

Summary of Existing Conditions

- Active Directory accounts were not disabled within 24 hours of an employee ending employment with the Riverside County Information Technology department. When an account is not closed immediately after employment has ended, there is a security risk to the information maintained in the systems used by the department.

- Disposed data devices did not have an Electronic Liability Surplus and Release Form to attest the devices were wiped clean of county data. Proper data destruction is an effective way to ensure sensitive data on devices becomes inaccessible and lowers the likelihood of a data breach.

Summary of Improvement Opportunities

- Ensure compliance with County of Riverside Information Security Standard v1.0, Section 4.1, *Account and Access Management*, by disabling Active Directory accounts on the day of an employee's termination or transfer from the department.

- Develop policies and procedures to ensure the disabling of Active Directory accounts are requested and approved within 24 hours of an employee ending employment with the department.

- Ensure compliance with RCIT Capital Asset Management Procedures, *Capital Asset Disposition*, by completing an Electronic Surplus Liability and Release Form for every data device disposed of and attest that the device has been wiped clean of county data.

- Develop a process to ensure an Electronic Surplus Liability and Release Form is completed for every data device to attest that the device has been wiped clean of county data.

Audit Conclusion

Based upon the results of our audit, we identified opportunities for improvement of internal controls relating to application controls and device disposal. However, we determined Riverside County Information Technology internal controls over software

licensing maintenance processes provide reasonable assurance that its objectives relating to this area will be achieved. Reasonable assurance recognizes internal controls have inherent limitations, including cost, mistakes, and intentional efforts to bypass internal controls.

Application Controls

Background

Application controls within information systems ensure proper confidentiality, integrity, and availability to the data stored within the system. Authentication is a control which confirms a user's identity to provide access to a systems sensitive information. Sensitive information is any information that must be protected from unauthorized access to maintain the information security of an organization or an individual. Authentication is often achieved by using login credentials such as a username and password. Authentication relies on the presumption that the user is authorized to use the system and that only the user knows the login credentials to gain access.

Active Directory is a directory service which allows Information Technology and other managed departments to manage permissions and access to network resources, and linked data applications utilized by the department. When a user ends employment with the county, Information Technology is notified through the creation of help desk tickets to disable Active Directory to remove permissions and network access. These help desk tickets contain various workflow tasks such as disabling e-mail accounts, active directory, data/application systems access, badge access, reclaiming software licenses, and reclaiming any equipment that may have been issued to an employee. A help desk ticket is not closed until all tasks within have been completed by Information Technology personnel.

Objective

To verify the existence and adequacy of internal controls over county employee termination of access for data applications.

Audit Methodology

To accomplish these objectives, we:

- Obtained an understanding of County of Riverside Information Security Standard v1.0.
- Obtained an understanding of county information security standards.
- Conducted interviews and performed walk-throughs with department personnel.
- Performed testing on 60 sampled Information Technology managed department employees terminated within the review period of the audit.
- Performed testing on 12 sampled Information Technology employees terminated within the review period of the audit.
- Confirmed whether terminated employees had access to active directory and data applications.
- Verified whether active directory accounts and data application accounts were disabled within 24 hours for non-Information Technology employees
- Verified whether requests to disable active directory and application data access was requested in a timely manner for Information Technology employees ending employment.

Finding 1: Timely Termination of Access Rights to Data Applications

Three (25%) out of twelve terminated employees reviewed, active directory accounts were not disabled within 24 hours of an employee ending employment with Information Technology. The average time lapsed to disable active directory accounts was 7 days with the longest time lapsed being 8 days and the shortest being 5 days. County of Riverside Information Security Standard v1.0, Section 4.1, *Account and Access Management*, states, "Accounts for terminated or transferred employees shall be disabled or removed on the day of termination or transfer." Requests and approvals to disable Active Directory are not created and approved timely after employees are no longer employed by the county. When an account is not closed immediately after employment has ended, there is a security risk to the information maintained in the systems used by the department.

Recommendation 1.1

Ensure compliance with County of Riverside Information Security Standard v1.0, Section 4.1, *Account and Access Management*, by disabling active directory accounts on the day of an employee's termination or transfer from the department.

Management's Response

"**Concur.** RCIT is assessing and modifying the current workflow to ensure compliance with Security Standard v1.0, Section 4.1, *Account and Access Management*, by disabling active directory accounts on the day of an employee's termination or transfer from the department. RCIT will perform internal self-audits in a timely manner to ensure this process is working properly."

Actual/Estimated Date of Corrective Action: August 31, 2022

Recommendation 1.2

Develop policies and procedures to ensure the disabling of active directory accounts are requested and approved within 24 hours of an employee ending employment with the department.

Management's Response

"**Concur.** RCIT is working to centralize the active directory account termination process within 24 hours of an employee ending employment with the department. RCIT will perform internal self-audits in a timely manner to make certain the process is working properly."

Actual/Estimated Date of Corrective Action: August 31, 2022

Device Disposal

Background

A data device can store electronic data in various formats. A data breach is an incident where information is stolen or removed from a system without the authorization of the system's owner. Devices can be sanitized of data to ensure no data breach occurs in several ways, which includes, but is not limited to, the following: Deleting/reformatting data, overwriting data, physical destruction of devices, and electronic shredding. Data destruction ensures data is safeguarded from unauthorized access.

County information is stored in data devices such as hard drives, storage drives, memory sticks, computers, printers, copiers, and servers. When data devices are no longer used by county departments, data devices must be disposed of properly to ensure that the county data stored within can no longer be accessed.

Objective

To verify the existence and adequacy of internal controls over disposal of data storage devices.

Audit Methodology

To accomplish these objectives, we:

- Obtained an understanding of the current RCIT Capital Asset Management Procedures.
- Conducted interviews and performed walk-throughs with department personnel.
- Obtained a listing of device disposals within the review period of the audit.
- Confirmed whether required documentation was completed for device disposals.
- Identified a total population of 28 device disposals classified as servers and storage systems.
- Selected a sample of 10 devices from the population of 28 device disposals classified as servers and storage systems.

- Confirmed whether required documentation attesting the storage devices were wiped clean to ensure no county data was stored when disposed.

Finding 2: Device Disposal

Seven (70%) out of ten device disposals sampled did not have an Electronic Liability Surplus and Release Form. RCIT Capital Asset Management Procedures, *Capital Asset Disposition*, states, "An Electronic Surplus Liability and Release Form must be completed when disposing of electronic devices such as hard drives, storage drives, memory sticks, computers, printers, copiers, and servers. This form will attest that all electronic items have been wiped clean and that these items do not have County data on them." The current processes do not ensure that an *"Electronic Surplus Liability and Release Form"* is completed to attest that disposed data devices have been sanitized of county data. Proper data destruction is an effective way to ensure sensitive data on devices becomes inaccessible and lowers the likelihood of a data breach.

Recommendation 2.1

Ensure compliance with RCIT Capital Asset Management Procedures, *Capital Asset Disposition*, by completing an *"Electronic Surplus Liability and Release Form"* for every data device that is disposed.

Management's Response

"Concur. In collaboration with Stakeholders, RCIT has implemented the recommendation to ensure compliance with the Capital Asset Disposition for every data device that is disposed. RCIT has created a fillable "Electronic Surplus Liability and Release Form." This form is included with the Surplus Property Transfer form, to ensure all data storage devices have been sanitized. The Digital Equity Program (DEP) staff have been trained to ensure both the surplus form and the fillable Electronic Surplus Liability and Release Form are completed and provided to the department upon removal of hard drive and/or confirmation of sanitization. The fillable Form was rolled out countywide on May 3, 2022."

Actual/Estimated Date of Corrective Action: May 3, 2022

Recommendation 2.2

Develop a process to ensure all data storage devices are wiped clean of county data when disposed.

Management's Response

"**Concur.** RCIT has developed a draft Digital Equity Program Procedure to ensure all data storage devices are wiped clean of county data when disposed. RCIT is in the process of refining the procedure."

Actual/Estimated Date of Corrective Action: October 1, 2022

Software Licensing Maintenance

Background

Software licenses are legally binding agreements that govern the use or redistribution of software. Software licenses provide rights to one or more copies of software without violating copyrights. License specifications might include, but not limited, to the following: number of times a software can be downloaded, costs of the software, cancellation terms, and duration of license agreement. Tracking of software licenses allows organizations to compare the number of purchased software licenses with the number currently installed on computers. Tracked license records can include the name of the software, product ID, license number, installation date, expiration date, and identifying information of the machines where software is installed.

Software licenses are purchased by Information Technology through a passthrough fund on behalf of county departments. When Information Technology purchases software licenses, county departments will be directly billed for the costs of the licenses and Information Technology is responsible for maintaining and tracking the licenses.

Objective

To verify the existence and adequacy of internal controls over maintenance of software licensing.

Audit Methodology

To accomplish these objectives, we:

- Conducted interviews and performed walk-throughs with department personnel.
- Obtained an inventory listing of software licenses for managed county departments.
- Performed testing on 30 sampled Information Technology passthrough fund expenditures.
- Confirmed whether county departments where accurately billed for software requested.
- Verified whether Information Technology was accurately reimbursed for the costs of acquiring software licenses for county departments.

Finding: None Noted

Based upon the results of our audit, we determined internal controls over software licensing processes provide reasonable assurance that its objective related to this area will be achieved.